Software Framework for Secure Online Transactions in Academic Institutions

Marylene S. Eder[1*] and Gerardo S. Doroja[2]
[1]College of Industrial and Information Technology
Mindanao University of Science and Technology
CM Recto Ave., Lapasan, Cagayan de Oro City, 9000 Philippines
**lhynshel@gmail.com*

[2]College of Computer Studies
Xavier University-Ateneo de Cagayan
Corrales Avenue, Cagayan de Oro City, 9000 Philippines

Date received: April 24, 2013
Revision accepted: July 25, 2013

Abstract

The rapidly growing interconnectivity of information system and the convergence of information technology that makes more pertinent data of the educational institutions generated and transmitted in the internet, allows wide distribution of digital data. It becomes much easier to edit, modify and duplicate digital information, therefore facing many threats. As a big security and privacy issue, it becomes necessary to find appropriate protection.

Universities and academic institutions in the Philippines encountered concerns about the security of its computing infrastructure and information resources; however, traditional security architectures are not effective for academic and research environments. This research aims to use a software development framework for integrating digital security requirements that is - practical and at the same time cost effective in the context of Philippine educational institutions.

In this study, software gateway was developed to address the four security issues namely confidentiality, authorization, non – repudiation and integrity. Results of the study show that adopting the software gateway enables colleges, universities, and other higher educational institutions in the Philippines to provide their clients with easy access to remote-transmitted, confidential documents through internet, ensures confidentiality and integrity of the transmitted data, ensures that only authorized persons or registered users can access the data, and that non-repudiation happens during transmission.

Keywords: software framework, confidentiality, authorization, non – repudiation

1. Introduction

Academic institutions deploy secure remote access technology, where appropriate, to secure the personal data of learners, staff, and any other authorized users (BECTA, 2009). Securing remote access systems and the personal data it contains involve multiple security issues. The rapid growth of the internet would now necessitate the use of some securing mechanism to protect users and data alike.

Nowadays, many applications need to transmit data to remote applications and computers securely. The four main stated security issues are confidentiality, authorization, non-repudiation, and integrity (Longstaff *et al*, 1997). Confidentiality ensures that only authorized parties can access the information while unauthorized users are to be denied access. Authorization guarantees that the user accessing the information is indeed the intended recipient to receive the service or information. Non-repudiation provides proof of the integrity and origin of data, and guarantees that senders and receivers cannot deny that they have transmitted or received information, respectively. Integrity ensures that the received information is the same as the transmitted information and has not been modified by others during transmission. These four mentioned issues are interdependent and must therefore be addressed systematically in the design of security systems. One such design scheme is the use of the Secure Sockets Layer (SSL) protocol that has been universally accepted in the World Wide Web for authenticated and encrypted communication between clients and servers (Mathew and Jacob, 2008).

Figure 1 shows how SSL protects confidential information using Public Key Infrastructure (PKI), an asymmetric cryptosystem (GC, 2011). Sensitive data is encrypted across public networks to achieve a high level of confidentiality. Primarily, PKI utilizes asymmetric cryptography that is considered more secure than symmetric cryptography. This is due to the fact that asymmetric algorithms use one key for encryption of data, and then a separate key for decryption. Asymmetric algorithms are stronger than symmetric algorithms because even if the encryption key is known in one direction, the third party still needs to know the other key in order to decrypt the message in the other direction.The primary benefit of asymmetric encryption is that both sides can spontaneously initiate a transaction without ever having met. This is achieved by the use of a public and private key pair. The public key of the entity is known to everyone and is used for encryption, whereas the private key of the entity remains secret and is used for decryption (EV SSL, 2011).

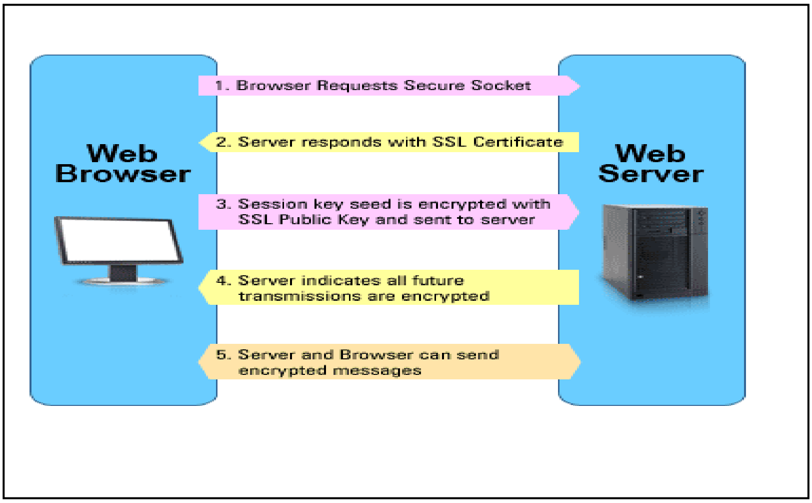

Web Browser
1. Browser Requests Secure Socket
2. Server responds with SSL Certificate
3. Session key seed is encrypted with SSL Public Key and sent to server
4. Server indicates all future transmissions are encrypted
5. Server and Browser can send encrypted messages
Web Server

Figure 1. An illustration on how SSL works using public key infrastructure

The Philippine Electronic Commerce Act (COP, 2000) provides for the recognition and use of electronic commercial and non-commercial transactions and documents, penalties for unlawful use thereof and for other purposes. An electronic document shall be regarded as the equivalent of an original document under the Best Evidence Rule if it is a printout or output readable by sight or other means, shown to reflect the data accurately.

As stated in Philippines Rules of Court on Electronic Evidence (SC, 2001), electronic documents are considered as functional equivalent of paper-based documents. Whenever a rule of evidence refers to the term of writing, document, record, instrument, memorandum or any other form of writing, such term shall be deemed to include an electronic document as defined in these rules.

As the information relies on security, cryptography plays the central role in an information security plan. Cryptography is the science or study of the techniques of secret writing, especially code and cipher systems, methods that use key based encryption and decryption technique (Brayton, 2006). Encryption is the art of turning a plain text message written by a sender to a ciphertext or encrypted message which is then sent on to a recipient. Modern computer-based encryption is done by an algorithm, which is generally publicly available to anyone, and a secret encryption key. For good encryption algorithms, it is nearly impossible to decrypt the ciphertext, i.e., recover the original plaintext message from the ciphertext without the correct key. Before being able to encrypt or decrypt, one must generate the key pair required for the encryption and decryption (Mathew and Jacob, 2010).

Software frameworks include support programs, compilers, code libraries, an Application Programming Interface (API) and tool sets that bring together all the different components to enable development of a project or solution. OpenSSL is an open source implementation of the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols (Moeller, 2011). The core library implements the basic cryptographic functions and provides various utility functions.

Due to the growing use of online technology for transactions in academic institutions, this paper proposes a software framework for a secure online local transaction in academic institutions in the Philippines that may be used in a security gateway to protect data passing through the internet against malicious intruders.

Figure 2 demonstrates the security gateway, where the message is made secured before passing through the internet. There are two basic kinds of cryptographic transformation; (a) the single key or symmetric cryptography where it uses the same key both encryption and decryption; and, (b) the two key (pair) or public key or asymmetric cryptography where the one key encrypts and made public, while the other decrypts, and is kept secret. An asymmetric cryptography or public-key cryptography is used in developing the application programming interface proposed in this study, where a pair of keys is used to encrypt and decrypt a message so that it arrives securely. Any other user who wants to send an encrypted message can get the intended recipient's public key from a public directory. The administrator uses the public key to encrypt the message, and sends it to the intended recipients. When the recipients get the message, they decrypt it with their respective private keys, in which no one else should have access to.

2. Methodology

In this study, a software framework was carefully designed to enable the use of encryption technology in ensuring confidentiality, authorization, non -

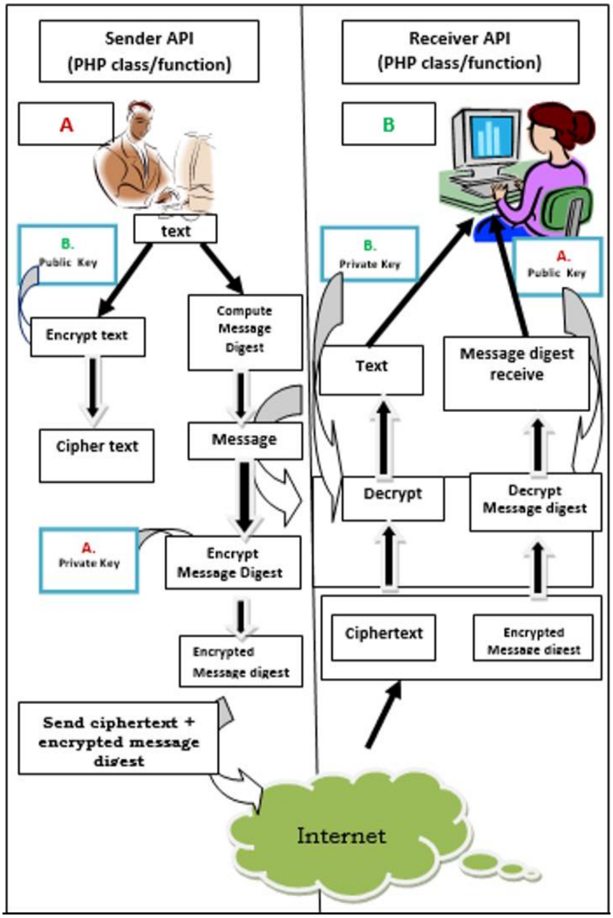


Figure 2. An Illustration of a security gateway using software framework

repudiation and integrity. The design is to develop a software framework for integrating digital security requirements that is – practical and at the same time cost effective in the Philippine educational institutions into the program development process.

2.1 Design of the Software Framework

2.1.1 Analysis

The record-in-charge of the registrar’s and the assessment’s office were interviewed in order to determine the transactions that need to be secured before being sent to the remote users. These transactions include transcript of records, honorable dismissal, report of grades, and statement of accounts. These files need to be secured before being sent to its remote users through the internet.

2.1.2 Design of the database

Centralized databases of the API for the key generation, and registered students information was designed. The number of tables to be created and the fields to be included in the table were initially decided. There were thirteen (13) fields in the table, namely, id, name, username, email, password, usertype, block, sendEmail, gid, registerDate, lastvisitDate, activation and params. The table name is jos_user.

2.1.3 Key Generation

Figure 3 illustrates how key generation is done. In this approach, key generation is achieved using Open SSL function. Certain algorithm is used in generating a key. Two keys are generated namely public and private key. After the key is generated, it will automatically be saved in the database using MySql.

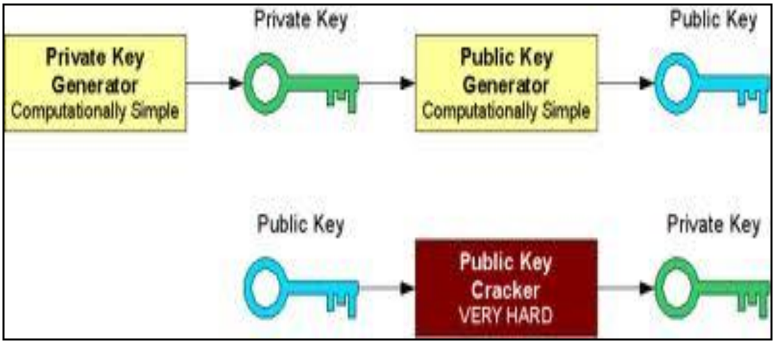


Figure 3. Diagram illustrating key generation

A user is registered first in the security gateway before a key is produced. A private and public key are produced in generating a key. After producing a key, it is then automatically saved in the database of the security gateway. The private key is given to the user while the public key remains in the gateway.

2.1.4 Design for Confidentiality of the Message

Figure 4 demonstrates confidentiality scheme. To ensure confidentiality of the message, the sender encrypts the messages using the public key of the receiver but only the holder of the paired private key can decrypt. Security depends on the secrecy of that private key. The private key is then saved to a flash disk or any removable disk of the registered recipient or student of the school.

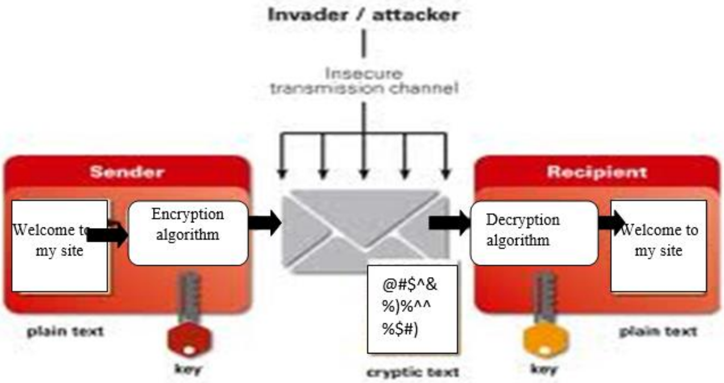


Figure 4. Diagram illustrating the confidentiality of the message

Figure 5 illustrates how integrity and authentication of the message is secured. To achieve this, signature schemes were done through the private key used to sign a message; but anyone can check the signature using the public key. Validity depends on the private key security. This process prevents unauthorized persons to access the message.

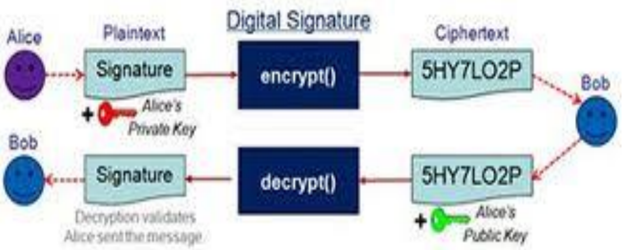


Figure 5. Diagram illustrating how authorization of the message is done

Figure 6 shows how integrity of the message is achieved. In order to provide data integrity, any message could be simply encrypted. To modify the data content of a message, the attacker would have to be in possesion of the the private key (in asymmetric systems). However, encryption systems use complex mathematical functions, and therefore consume large CPU resources. Hence, to encrypt all messages may incur unacceptably high overheads and especially frustrating where data confidentiality is not a requirement. Fortunately, other techniques can be used to reduce this load. The most common is a lightweight procedure called a one-way hash (also simply called a hash), or more commonly a message digest. The hash or digest algorithm creates a unique and relatively small fixed-size block of data (irrespective of the original message length) that cannot be reversed. The messages being sent typically include both the plain text (unencrypted) and a digest of the message. The hash algorithm is applied to the received plain text and if the result matches the message digest, this means the received data was not altered. The message digest is, in some sense, similar in concept to a checksum but has significantly different mathematical properties.

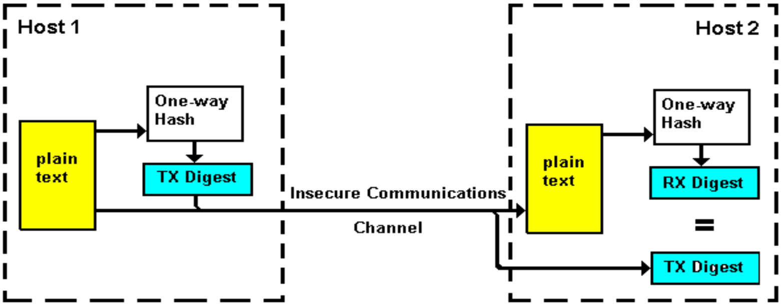


Figure 6. An illustration of how integrity of the message is achieved

Figure 7 illustrates how the non-repudiation of the message is achieved. Non-repudiation is the assurance that someone cannot deny something. On the Internet, a digital signature is used not only to ensure that a message or document has been electronically signed by the person that purported to sign the document, but also, since a digital signature can only be created by one person, to ensure that a person cannot later deny that they furnished the signature.

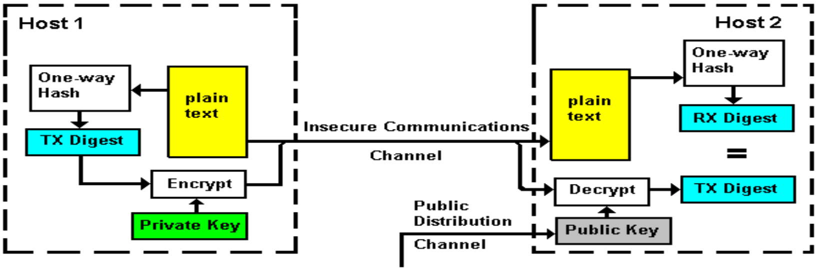


Figure 7. Diagram for non - repudiation of the message

2.2 Development of the Software Framework

2.2.1 Identification of Built-in Libraries for Software Framework

The software used in Application Programming Interface includes Joomla, OpenSSL Functions, XAMPP, and Notepad++.

Joomla is a free and open source content management system (CMS) for publishing content on the World Wide Web and intranets. It comprises a model–view–controller (MVC) Web application framework that can also be used independently. (JQC, 2011)

MySQL is a free, open source database program. It is often used for web site applications and in web site design. It can be used to create and manipulate information contained in databases by adding, removing, and modifying information in the database. (MySql, 2011)

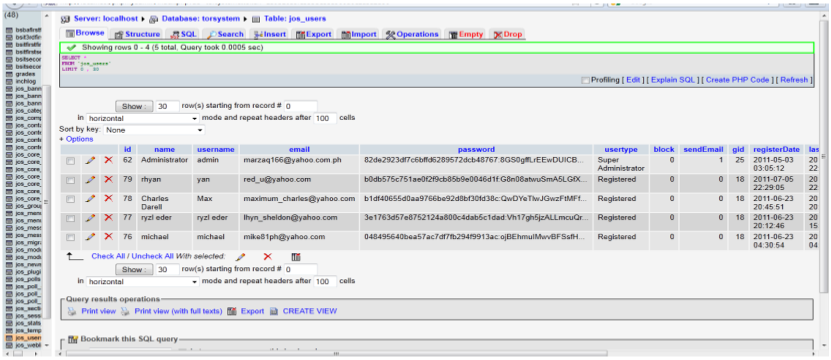
OpenSSL functions are used for key generation and verification of signatures and for sealing (encrypting) and opening (decrypting) data. (Moeller, 2011)

XAMPP is a small and light Apache distribution containing the most common web development technologies in a single package. Its contents, small size, and portability make it the ideal tool for developing and testing applications in PHP and MySQL. (Dvorski, 2007)

Notepad++ is a free source code editor and a text editor for Windows. It is a tabbed editing, which allows working with multiple open files. (PS, 2011)

2.2.2 Creation of Database

A database is composed of one or more 'tables', each of which contains a list of fields. As shown in Figure 8, the database used in this study starts with a table called "jos_user". Each table in a database has one or more columns called fields. Each column holds a certain piece of information about each "thing" in the database.



Server: localhost ▸ Database: torsystem ▸ Table: jos_users
Browse
Structure
SQL
Search
Insert
Export
Import
Operations
Empty
Drop

✓ Showing rows 0 - 4 (5 total, Query took 0.0005 sec)

```
SELECT *
FROM `jos_users`
LIMIT 0 , 30
```

□ Profiling [Edit] [Explain SQL] [Create PHP Code] [Refresh]

Show : 30 row(s) starting from record # 0
in horizontal mode and repeat headers after 100 cells
Sort by key: None
+ Options

			id	name	username	email	password	usertype	block	sendEmail	gid	registerDate	las
□	✎	✕	62	Administrator	admin	marzaq166@yahoo.com.ph	82de2923df7c6bffd6289572dcb48767:8GS0gffLrEEwDUICB...	Super Administrator	0	1	25	2011-05-03 03:05:12	20 22
□	✎	✕	79	rhyan	yan	red_u@yahoo.com	b0db575c751ae0f2f9cb85b9e0046d1f:G8n08atwuSmA5LGfX...	Registered	0	0	18	2011-07-05 22:29:05	20 22
□	✎	✕	78	Charles Darell	Max	maximum_charles@yahoo.com	b1df40655d0aa9766be92d8bf30fd38c:QwDYeTlwJGwzFtMFf...	Registered	0	0	18	2011-06-23 20:45:51	20 20
□	✎	✕	77	ryzl eder	ryzl eder	lhyn_sheldon@yahoo.com	3e1763d57e8752124a800c4dab5c1dad:Vh17gh5jzALLmcuQr...	Registered	0	0	18	2011-06-23 20:12:46	20 15
□	✎	✕	76	michael	michael	mike81ph@yahoo.com	048495640bea57ac7df7fb294f9913ac:ojBEhmulMwvBFSsfH...	Registered	0	0	18	2011-06-23 04:30:54	20 04

Show : 30 row(s) starting from record # 0
in horizontal mode and repeat headers after 100 cells

Figure 8. Diagram on the creation of the database

The "jos_user" table is composed of columns for the text of id, name, username, email, password, usertype, block, sendEmail, gid, registerDate, lastvisitDate, activation and params added to the database. Each of the information stored in this table is then referred to as a 'row' in the table. Each row contains the record of each of the registered users.

2.2.3 Encryption

OpenSSL functions and PHP classes and functions were used in developing the security gateway for encryption and decryption. The sender creates a ciphertext message by encrypting the plaintext message with an asymmetric encryption algorithm and the recipient's public key using openSSL functions. The sender sends the ciphertext message to the recipient. Only the holder of the paired private key can decrypt the messages. The registered user decrypts the ciphertext message back to plaintext using the private key that corresponds to the public key used to encrypt the message. The security depends on the secrecy of that private key given to the registered student.

2.2.4 Authorization and Digital Signature

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient reason to believe that the message has been created by a known sender, and has not been altered in transit. Digital signatures are commonly used for software distribution, financial transactions, and in cases where it is important to detect forgery and tampering.

The electronics/equivalent of the document and finger print pair is the message and digest pair. To preserve the integrity of a message, MD5/SHA1 are used to encrypt the message digest. The message is then passed through an algorithm called hash function. Digital Signature using hashed function creates a compressed image of the message that can be used as a fingerprint.

2.2.5 Testing and Debugging

In order to ensure accuracy and workability of the program, testing was conducted. During testing, some errors have been encountered. Debugging has been made in order to address these problems.

3. Results and Discussion

3.1 Analysis

Table 1 shows the transactions needed to be secured. After analysis, it was found out that the transactions that need file security before being sent to other users through internet are as follows: transcript of records, honorable dismissal, and report of grades and statement of account. These transactions are confidential documents of the school and only bonafide students and authorized users have the right to view and read the file over the internet.

3.2 Design of the Software Framework

In order to come up with an efficient security gateway, which is the focus of the study, the security requirements of the files namely confidentiality, authorization, non-repudiation and integrity were addressed.

Table 1. Descriptions of the transactions needed to be secured

Documents	Description	Security Requirements Needed
1. Transcript of Record	A copy of a student's permanent academic record which usually means all courses taken, all grades received, all honors received and degrees conferred to a student	Encryption Confidentiality Authorization Non repudiation
2. Honorable Dismissal	A certification issued to the student stating the voluntary withdrawal from the University with the consent of the University Registrar or his representative.	Encryption Authorization Integrity
3. Report of Grades	A partial list of grades of a student taken during the last semester enrolled	Encryption Authorization Integrity
4. Statement of Account	Statement displays prior term balances, tuition, fees, and any charges for every term of school year.	Encryption Confidentiality Authorization Non repudiation

Encryption is required to address the problem of security. In designing the security gateway, the software used was MySQL for database and openSSL function for key generation. MySQL was chosen because it is a free open source relational database management system and can be used for a variety of applications most commonly on Web servers. In generating a key, openSSL function was used for it provides various encryption and decryption algorithm that can be of great help for the said security requirements of the files.

Figure 9 shows the modular design of the Application Programming Interface (API). Client Program is where the clients access their files through net. The function *secure_file* () encrypts *data* with public *key* and stores the result into *crypted*. Encrypted data is decrypted via the function *read_file,* e.g. the function *read_file* is used to encrypt message which can then be read only by the owner of the private key. It can be also used to store secure data in database. The function *key()* generates a new private and public key pair. The public component of the key is obtained using the function *openssl_pkey_get_public()*. The function *get_cipher*() is used to get the name of the specified cipher. This function takes the cipher number as an argument or takes the cipher name as an argument and returns the name of the cipher or FALSE, if the cipher does not exist. *OpenSSL read_file* () decrypts *data* that was previous encrypted via *function secure_file()* and stores the result into *decrypted*. This function is used to decrypt data only for the intended or authorized person.

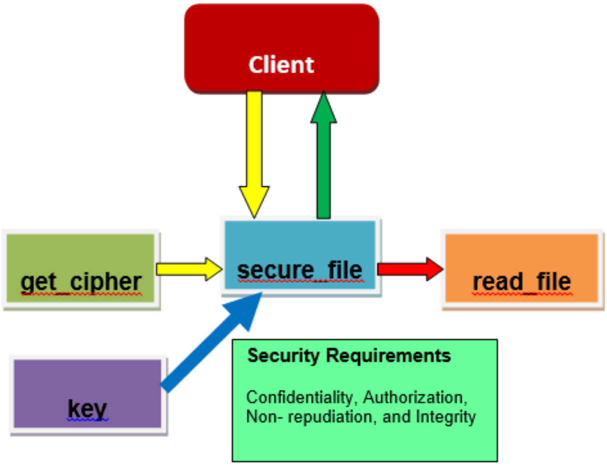
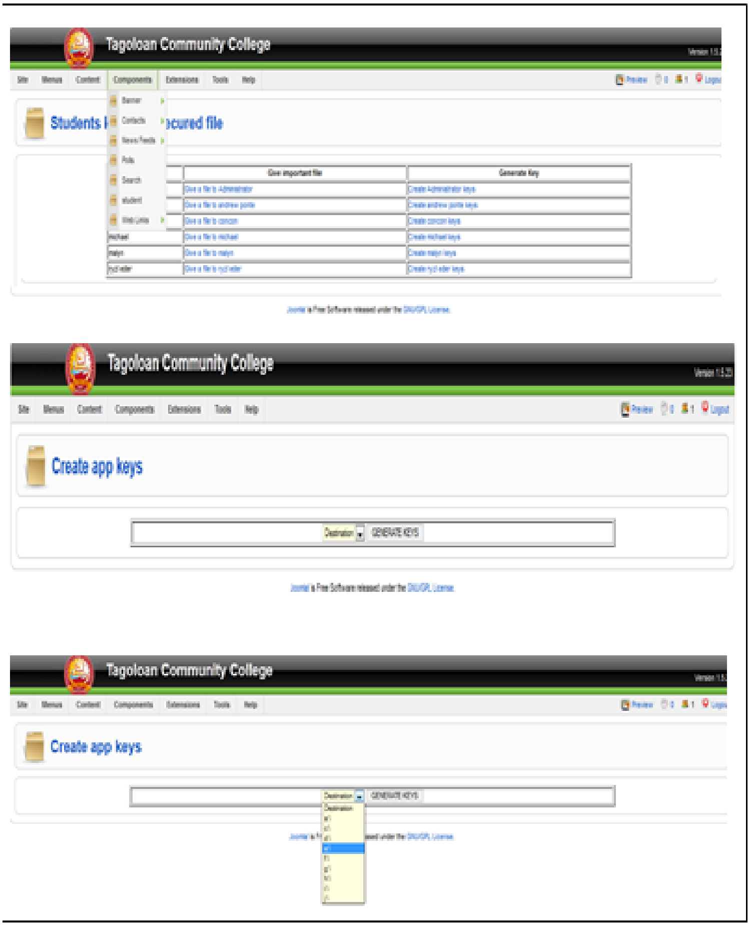

Client
get_cipher
secure_file
read_file
key
Security Requirements
Confidentiality, Authorization, Non- repudiation, and Integrity

Figure 9. Modular design of the API

3.2.1 Key Generation

Figure 10 illustrates the key generation process. In this study, key generation is designed using OpenSSL function. In order to generate public and privatekey, one must first click on *components* on the main page, then *student, give (username) key* and *destination*.



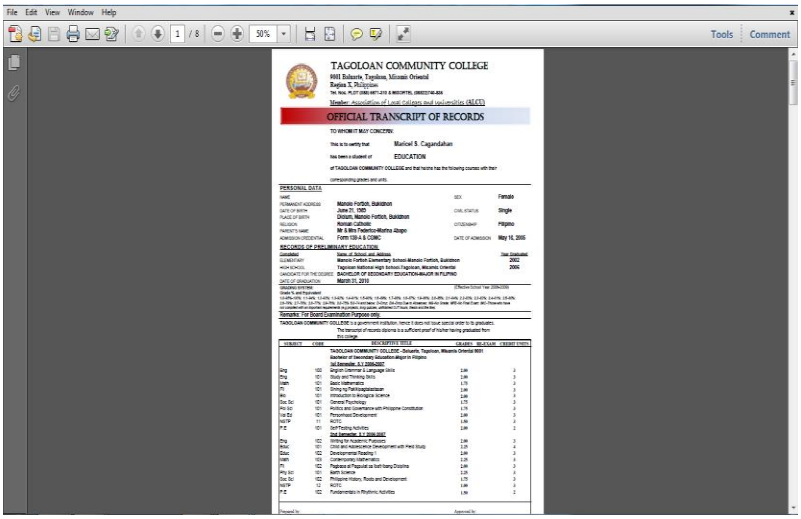
	Give important file	Generate Key
	Give a file to Administrator	Create Administrator keys
	Give a file to andrew ponte	Create andrew ponte keys
	Give a file to concon	Create concon keys
michael	Give a file to michael	Create michael keys
malyn	Give a file to malyn	Create malyn keys
nyd eder	Give a file to nyd eder	Create nyd eder keys

Figure 10. Key generation process

3.2.2 Confidentiality, Authorization, Non-repudiation and Integrity Considerations in the Design

Figure 11 shows an example of an original file to be sent by a sender to a registered recipient. Standard algorithm for encryption method performs a series of mathematical operations on the original message.

Using the public key of the receiver, it encrypts the original file resulting to a ciphertext. Figure 12 shows the resulting ciphertext. Ciphertext is an output file after encryption process.



TAGOLOAN COMMUNITY COLLEGE
9001 Balurate, Tagoloan, Misamis Oriental
Region X, Philippines
Tel. Nos. PLDT (088) 6871-010 & MISORTEL (08822)740-806
Member: Association of Local Colleges and Universities (ALCU)

OFFICIAL TRANSCRIPT OF RECORDS

TO WHOM IT MAY CONCERN:

This is to certify that Maricel S. Cagandahan

has been a student of EDUCATION

of TAGOLOAN COMMUNITY COLLEGE and that he/she has the following courses with their corresponding grades and units.

PERSONAL DATA

NAME		SEX	Female
PERMANENT ADDRESS	Manolo Fortich, Bukidnon		
DATE OF BIRTH	June 21, 1989	CIVIL STATUS	Single
PLACE OF BIRTH	Dicium, Manolo Fortich, Bukidnon		
RELIGION	Roman Catholic	CITIZENSHIP	Filipino
PARENT'S NAME	Mr & Mrs Federico-Marina Abapo		
ADMISSION CREDENTIAL	Form 138-A & CGMC	DATE OF ADMISSION	May 16, 2005

RECORDS OF PRELIMINARY EDUCATION

Completed	Name of School and Address	Year Graduated
ELEMENTARY	Manolo Fortich Elementary School-Manolo Fortich, Bukidnon	2002
HIGH SCHOOL	Tagoloan National High School-Tagoloan, Misamis Oriental	2006
CANDIDATE FOR THE DEGREE	BACHELOR OF SECONDARY EDUCATION-MAJOR IN FILIPINO	
DATE OF GRADUATION	March 31, 2010	

GRADING SYSTEM: (Effective School Year 2009-2010)
Grade % and Equivalent
[illegible]

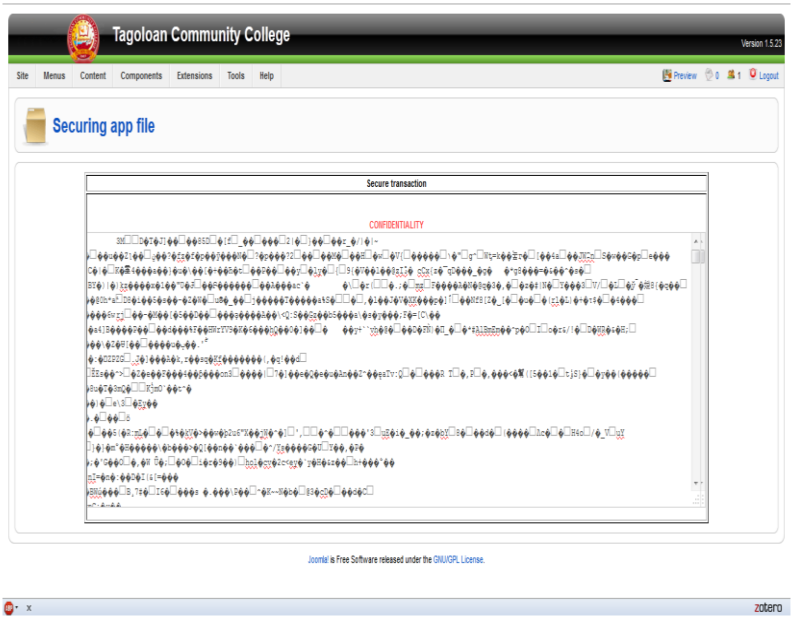
Remarks: For Board Examination Purpose only.

TAGOLOAN COMMUNITY COLLEGE is a government institution, hence it does not issue special order to its graduates. The transcript of records diploma is a sufficient proof of his/her having graduated from this college.

SUBJECT	CODE	DESCRIPTIVE TITLE	GRADES	RE-EXAM	CREDIT UNITS
		TAGOLOAN COMMUNITY COLLEGE - Baluarte, Tagoloan, Misamis Oriental 9001			
		Bachelor of Secondary Education-Major in Filipino			
		1st Semester, S.Y 2006-2007			
Eng	100	English Grammar & Language Skills	2.00		3
Eng	101	Study and Thinking Skills	2.00		3
Math	101	Basic Mathematics	1.75		3
Fil	101	Sining ng Pakikipagtalastasan	2.00		3
Bio	101	Introduction to Biological Science	2.00		3
Soc Sci	101	General Psychology	1.75		3
Pol Sci	101	Politics and Governance with Philippine Constitution	1.75		3
Val Ed	101	Personhood Development	2.00		3
NSTP	11	ROTC	1.50		3
P.E	101	Self-Testing Activities	2.00		2
		2nd Semester, S.Y 2006-2007			
Eng	102	Writing for Academic Purposes	2.00		3
Educ	101	Child and Adolescence Development with Field Study	2.25		4
Educ	102	Developmental Reading 1	2.00		3
Math	103	Contemporary Mathematics	2.25		3
Fil	102	Pagbasa at Pagsulat sa Iba't-ibang Disiplina	2.00		3
Phy Sci	101	Earth Science	2.25		3
Soc Sci	102	Philippine History, Roots and Development	1.75		3
NSTP	12	ROTC	1.00		3
P.E	102	Fundamentals in Rhythmic Activities	1.50		2

Prepared by: Approved by:

Figure 11. A copy of the original file from the sender



Secure transaction

CONFIDENTIALITY

[illegible]

Joomla! is Free Software released under the GNU/GPL License.

Figure 12. Resulting screen after the secure and display ciphertext to the public is chosen

Figure 13 shows how authorization issue is addressed in the security gateway. Authorization refers to mechanisms that decide when a user is *authorized* to perform a certain task. The hash or digest algorithm creates a unique and relatively small fixed-size block of data (irrespective of the original message length) that cannot be reversed. The messages being sent typically include both the plain text (unencrypted) and a digest of the message. The hash algorithm is applied to the received plain text and if the result matches the message digest, this means the received data was not altered. The message digest is, in some senses, similar in concept to a checksum but has significantly different mathematical properties (SG, 2011).

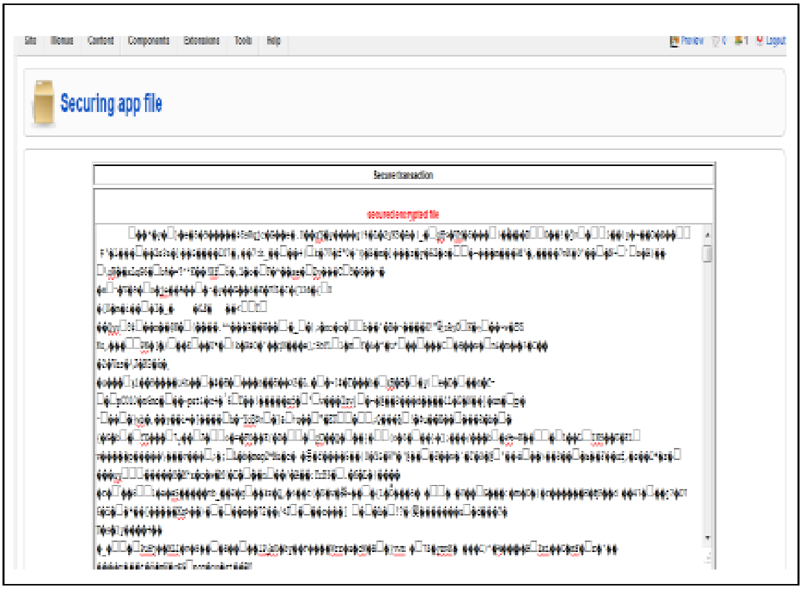
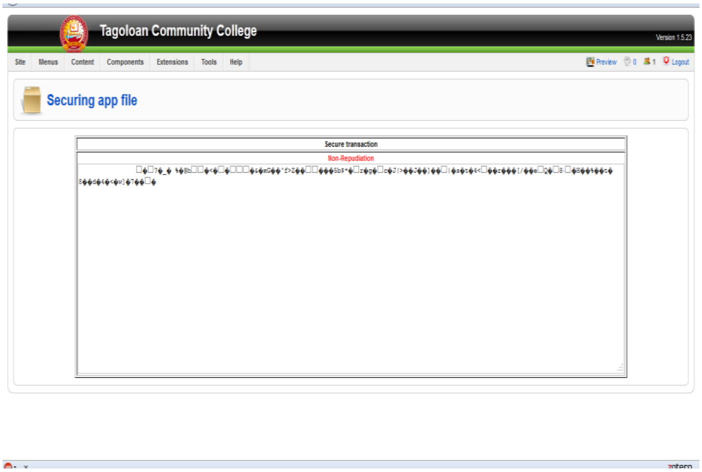


Figure 13. Screenshot showing how authorization is achieved

Figure 14 shows a screenshot demonstrating how non-repudiation is addressed. The file to be transmitted is again hashed to create a message digest using MD5 to ensure data integrity. The resulting message digest is then encrypted using the private key of the sender. Both the plain-text message and the encrypted digest are sent to the other party assured (SG, 2011).



Securing app file

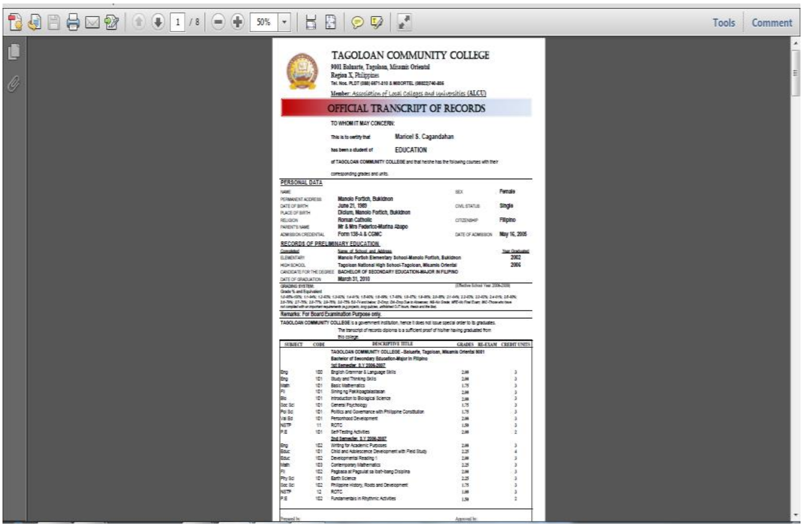
Secure transaction

Non-Repudiation

[illegible]

Figure 14. Screenshot showing how non-repudiation is addressed

Figure 15 demonstrates how the integrity of the message is ensured and the authenticity of the message is maintained by preventing any unauthorized persons to access the message. The receiver decrypts the message digest using the public key of the sender, applies the hash algorithm to the plain-text data, and if the results match, then both the authenticity of the sender and the integrity of the data are assured (SG, 2011).



TAGOLOAN COMMUNITY COLLEGE
9001 Baluarte, Tagoloan, Misamis Oriental
Region X, Philippines
Tel. Nos. PLDT (088) 6871-310 & MISORTEL (08822)740-856
Member: Association of Local Colleges and Universities (ALCU)

OFFICIAL TRANSCRIPT OF RECORDS

TO WHOM IT MAY CONCERN:

This is to certify that Maricel S. Cagandahan

has been a student of EDUCATION

of TAGOLOAN COMMUNITY COLLEGE and that he/she has the following courses with their corresponding grades and units.

PERSONAL DATA

NAME		SEX	Female
PERMANENT ADDRESS	Manolo Fortich, Bukidnon		
DATE OF BIRTH	June 21, 1989	CIVIL STATUS	Single
PLACE OF BIRTH	Dicium, Manolo Fortich, Bukidnon		
RELIGION	Roman Catholic	CITIZENSHIP	Filipino
PARENTS NAME	Mr & Mrs Federico-Marina Abapo		
ADMISSION CREDENTIAL	Form 138-A & CGMC	DATE OF ADMISSION	May 16, 2005

RECORDS OF PRELIMINARY EDUCATION

Completed	Name of School and Address	Year Graduated
ELEMENTARY	Manolo Fortich Elementary School-Manolo Fortich, Bukidnon	2002
HIGH SCHOOL	Tagoloan National High School-Tagoloan, Misamis Oriental	2006
CANDIDATE FOR THE DEGREE	BACHELOR OF SECONDARY EDUCATION-MAJOR IN FILIPINO	
DATE OF GRADUATION	March 31, 2010	

GRADING SYSTEM: (Effective School Year 2008-2009)
Grade % and Equivalent
1.0-95%-100%; 1.1-94%; 1.2-93%; 1.3-92%; 1.4-91%; 1.5-90%; 1.6-89%; 1.7-88%; 1.8-87%; 1.9-86%; 2.0-85%; 2.1-84%; 2.2-83%; 2.3-82%; 2.4-81%; 2.5-80%; 2.6-79%; 2.7-78%; 2.8-77%; 2.9-76%; 3.0-75%; 5.0-74 and below; D-Drop; DA-Drop Due to Absences; NG-No Grade; NFE-No Final Exam; INC-Those who have not complied with an important requirements (e.g.projects, long quizzes, unfinished OJT hours, thesis and the like)

Remarks: For Board Examination Purpose only.

TAGOLOAN COMMUNITY COLLEGE is a government institution, hence it does not issue special order to its graduates.
The transcript of records diploma is a sufficient proof of his/her having graduated from this college.

SUBJECT	CODE	DESCRIPTIVE TITLE	GRADES	RE-EXAM	CREDIT UNITS
		TAGOLOAN COMMUNITY COLLEGE - Baluarte, Tagoloan, Misamis Oriental 9001			
		Bachelor of Secondary Education-Major in Filipino			
		1st Semester, S.Y 2006-2007			
Eng	100	English Grammar & Language Skills	2.00		3
Eng	101	Study and Thinking Skills	2.00		3
Math	101	Basic Mathematics	1.75		3
Fil	101	Sining ng Pakikipagtalastasan	2.00		3
Bio	101	Introduction to Biological Science	2.00		3
Soc Sci	101	General Psychology	1.75		3
Pol Sci	101	Politics and Governance with Philippine Constitution	1.75		3
Val Ed	101	Personhood Development	2.00		3
NSTP	11	ROTC	1.50		3
P.E	101	Self-Testing Activities	2.00		2
		2nd Semester, S.Y 2006-2007			
Eng	102	Writing for Academic Purposes	2.00		3
Educ	101	Child and Adolescence Development with Field Study	2.25		4
Educ	102	Developmental Reading 1	2.00		3
Math	103	Contemporary Mathematics	2.25		3
Fil	102	Pagbasa at Pagsulat sa Iba't-ibang Disiplina	2.00		3
Phy Sci	101	Earth Science	2.25		3
Soc Sci	102	Philippine History, Roots and Development	1.75		3
NSTP	12	ROTC	1.00		3
P.E	102	Fundamentals in Rhythmic Activities	1.50		2

Prepared by: Approved by:

Figure 15. Screenshot showing how integrity is achieved

4. Conclusion and Recommendation

Software gateway is developed for integrating digital security requirements that is - practical and at the same time cost effective in the context of Philippine educational institutions and to address the four security issues namely *confidentiality, authorization, non – repudiation and integrity.* As usual scheme, this system supports the information dissemination and allows the users to develop and test insecure software protocols while protecting information and computing resources. Based on the findings of the study, it is concluded that adopting the software gateway enables colleges, universities, and other higher educational institutions to provide their clients (parents, students, staff and other authorized and registered users) with easy access to remote-transmitted, confidential documents and or files (transcript of record, honorable dismissal, report of grades, and statement of account) through the internet, while ensuring confidentiality and integrity of the transmitted data, that only authorized persons or registered users can access the transmitted data, and that non-repudiation happens during data transmission.

To further enhance the proposed study, it is recommended to improve the security gateway by adding a module for error handling. Error handling refers to the anticipation, detection, and resolution of programming, application, and communications errors. Logging or audit trail of the user profile should also be included for the location of the user from usual location to different location. Audit trails are useful both for maintaining security and for recovering lost transactions. Third party key management is also necessary for organization that will handle or manage the key. Finally, use of continuous scaling or Likert scale method in designing the evaluation questionnaire (not simply a yes – no question) is essential for better evaluation results.

5. References

BECTA, (2009). Good practice in information handling: Secure remote access, http://www.becta.org.uk/schools/datasecurity

Brayton, J, Finneman, A, Turajski, N and Wiltsey, S, (2006) Public Key Infrastructure, http:// searchsecurity.techtarget.com/ definition

COP (2000). Republic Act No. 8792: An Act Providing for the Recognition and Use of Electronic Commerece and Non – Commercial Transactions and Documents, Penalties for Unlawful Use Thereof and for other Purpose, Congress of the Philippines, Metro Manila, Philippines, June 14, 2000.

Dvorski, D, (2007) Installing, Configuring, and Developing with XAMPP, http://dalibor.dvorski.net/downloads/docs/InstallingConfiguringDevelopingWithXAMPP.pdf

EV SSL, (2011) Extended Validation SSL Certificate. The Next Generation High Assurance Certificate, http://www.evsslcertificate .com/ssl/description-ssl.html

GC, (2011) A simple Guide to Cryptography, http://msdn. microsoft.com/en-us/library/aa480359.aspx

JQC (2011) Joomla Quietly Crosses 23 Million Downloads, Now Powering Over 2,600 Government Sites. TechCrunch, http://en.wikipedia.org/wiki/Joomla

Longstaff, T, Ellis, J, Lipson H, McMillan, R, Hutz-Pesante L and Simmel D (1997). Security of the Internet, The Froehlich/Kent Encyclopedia of Telecommunications, Vol. 15, Marcel Dekker, New York, pp. 231-255

Mathew, S and K. P Jacob. (2008). Use of Novel Algorithms MAJE4 and MACJER-320 for Achieving Confidentiality and Message Authentication in SSL & TLS. World Academy of Science, Engineering and Technology, World Academy of Science, Engineering and Technology 39 200, 2008.

Moeller, B. (2011) Open SSL, http://en.wikipedia.org/ wiki/OpenSSL

MySQL, (2011), http://www.hooverwebdesign.com/definition-of-mysql.html

PS, (2011) SourceForge.net: Project Statistics for Notepad++. SourceForge.net., http://en.wikipedia.org/wiki/Notepad%2B%2B

SC (2001) Rules on Electronic Evidence A.M. no. 01-7-01-sc.Committee on the Revision of the Rules of Court, Senate Congress, Metro Manila, Philippines, June 18, 2001

SG, (2011) Survival Guide – Encryption, Authentication, http://www.zytrax.com/tech/survival/encryption.html